Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. – 4. (Canceled)

5. (Currently amended) A tamper-resistant processing method comprising the steps of:

(a) deciding ~~which step is to be selected out of the following steps (b) and (c) for each processing of one operation unit;~~

~~(b) after transferring~~ whether to first transfer one operation unit in the bit pattern of data A in a memory ~~in order of bit sequence of said data A~~ to a first register ~~R1, transferring~~ R1 and then to transfer one operation unit in the bit pattern of data B in the memory ~~in order of bit sequence of said data B~~ to a second register ~~R2;~~ R2, or to first transfer

~~(c) after transferring~~ one operation unit in the bit pattern of said data B ~~in order of bit sequence of said data B~~ to said second register ~~R2, transferring~~ R2 and then to transfer one operation unit in the bit pattern in said data A ~~in order of bit sequence of said data A~~ to said first register R1;

~~(d)~~ (b) executing a predetermined arithmetic operation on the contents of said first register R1 and the contents of said second register R2;

~~(e)~~ (c) storing the result of said arithmetic operation in the memory,

~~(f)~~ (d) repeating the steps from (a) through ~~(e)~~ (c) until said arithmetic operation for said data A and said data B is finished.

6. (Currently amended) A tamper-resistant processing method comprising the steps of:

(a) deciding ~~which step is to be selected out of the following steps (b) and (c) for each processing of one operation unit;~~

~~(b) after transferring~~ whether to first transfer one operation unit of data A in a memory ~~in order of bit sequence of said data A~~ to a first register ~~R1, transferring~~ R1 and then to transfer one operation unit of data B in the memory ~~in order of bit sequence of said data B~~ to a second register ~~R2;~~

~~(c) after transferring~~ R2, or to first transfer said one operation unit of the data A ~~in order of bit sequence of said data A~~ to said second register ~~R2, transferring~~ R2 and then to transfer said one operation unit of the data B ~~in order of bit sequence of said data B~~ to said first register R1;

~~(d)~~ (b) executing a predetermined arithmetic operation on the contents of said first register R1 and on the contents of said second register R2;

~~(e)~~ (c) storing the result of said arithmetic operation in the memory;

~~(f)~~ (d) repeating the steps from (a) through ~~(e)~~ (c) until said arithmetic operation on said data A and said data B is finished.

7. (Currently amended) A tamper-resistant processing method of claim 6 wherein ~~which one out of said steps (b) and (c)~~ whether to first transfer one

operation unit of the data A to said first register R1 or to said second register R2 ~~is to be processed~~ is determined with the use of a generated random number.

8. (Original) A tamper-resistant processing method of claim 6 wherein said predetermined arithmetic operation is the operation for an arithmetic sum.

9. (Original) A tamper-resistant processing method of claim 6 wherein said predetermined arithmetic operation is the operation for an arithmetic product.

10. (Original) A tamper-resistant processing method of claim 6 wherein said predetermined arithmetic operation is any one of the logical sum OR, logical product AND, and exclusive logical sum EXOR.

11. – 13. (canceled)